基于 2D sine Logistic 混沌映射的医学图像频域加密算法 *

邓小鸿 [1]，梁涤青 [2]，刘惠文 [1]

(1. 江西理工大学 应用科学学院, 江西 赣州 341000; 2. 长沙理工大学 信息化建设与管理处, 长沙 410114)

摘 要：针对现有医学图像加密算法在加密效率和安全性上的不足，提出一种基于 2D sine Logistic 混沌映射的医学图像小波域加密算法。算法首先利用整数小波变换将医学图像从空域转换为频域，充分打破像素间的相关性；其次，利用 2D sine Logistic 混沌映射生成混沌序列，选取三级小波分级的低频系数 LL3 进行扩散和置乱加密，提高加密效率；并且将二级小波分解的中高频系数 HL2 和 LH2 进行扩散加密，解决加密图像中存在的明显轮廓问题；最后将加密后的小波系数进行小波逆变换得到加密图像。实验仿真结果表明，算法具有高安全性和加密效率，与现有空域方法相比，加密时间约为 1/40；与现有频域方法相比，在保证加密效率情况下具有更好的加密图像隐蔽性。

关键词：混沌映射；医学图像；数据加密；整数小波变换；隐蔽性

中图分类号：TP309.2 doi: 10.19734/j.issn.1001-3695.2018.07.0562

Medical image encryption algorithm in frequency domain base on 2D sine logistic chaotic mapping

Deng Xiaohong[1], Liang Diqing[2], Liu Huiwen[1]

(1. *College of Applied Science*, *Jiangxi University of Science & Technology*, *Ganzhou* Jiangxi 341000, *China*; 2. *Informatization Construction & Management Dept.* , *Changsha University of Science & Technology*, *Changsha* 410114, *China*)

Abstract: Aiming at the shortage of medical images encryption algorithm in efficiency and security, this paper proposed a novel medical image encryption algorithm in frequent domain based on 2D sine Logistic chaotic mapping. Firstly, the proposed algorithm used the integer wavelet transform of LeGall5/3 to transform medical image from frequent domain to spatial domain. In this way, the high correlation among pixels has disappeared. Then, the proposed algorithm utilized 2D sine logistic chaotic mapping to generate the chaotic sequences. In order to improve the encryption efficiency, this algorithm chose the low frequency coefficients of three-level decomposed to encrypt with chaotic diffusion and scrambling mechanism. In the same time, this algorithm also selected the medium-high frequency coefficients of two-level decomposed to encrypt by chaotic diffusion mechanism for solving the problem of obvious outline in encrypted image. Finally, this algorithm transformed the encrypted wavelet coefficients by the inverse integer wavelet transform and obtained the encrypted image. Experimental simulation results demonstrate that the proposed algorithm is able to protect medical images with low time complexity and a high security level. Compared with the existing spatial method, it reduces the encryption time by about 0.025 times. In addition, the proposed algorithm has better image imperceptibility as well as an excellent encryption efficiency compared to the existing frequent method.

Key words: chaotic mapping; medical image; data encryption; integer wavelet transform; imperceptibility

0 引言

随着“互联网+医疗”的不断发展,医学图像的在线传输变得越来越普遍。数字医学图像在临床医疗诊断中起着至关重要的作用，但由于其含有病人的重要隐私信息，其安全问题也受到研究者们的广泛关注[1~3]。在众多的安全保护方法中，加密仍然是对数据进行主动保护的有效方法。相比自然图像，医学图像具有数据量大、典型的分区域特征、高的像素相关性、直方图分布不均匀等特点，一些适用于自然图像的加密方法并不适应于医学图像，如传统的 ASE、3DES 等算法并不能满足大数据量的医学图像实时加密。混沌映射具有伪随机性、遍历性和初值敏感性等特点，根据混沌映射产生的混沌序列具有安全密钥的良好特性，混沌密码学逐渐成为密码学一个新的研究方向，利用混沌映射进行医学图像加密已经被研究者们证明具有高的安全性和加密效率[4~6]。

目前，基于混沌映射的医学图像加密算法可以分为两大类：基于空域和基于频域的方法，前者利用混沌映射生成的混沌序列对医学图像的像素进行加密，典型的方法如文献[7~9]。文献[7]设计了一个基于混沌映射的置乱与替换扩散架构用于医学图像加密，对所有像素进行异或加密后改变其位置，算法具有高的加密性能，但由于医学图像的数据量大，算法的加密效率不高。为了解决基于空域算法的加密效率问题，Moumen 等人[8]提出选取图像的部分像素进行加密，利用图着色理论选取图像中的部分像素进行混沌加密。Pareek 等人[9]根据医学图像的分区域特性，提出对医学图像的感兴趣区域（前景区域）进行混沌加密。但上述方法需要特征抽取、模式匹配和其他先验知识，降低了算法的可操作性，如感兴趣区域提取时需要对区域进行分割、由于区域的不规则

收稿日期：2018-07-25；**修回日期：**2018-08-31 **基金项目：**国家自然科学基金资助项目（61762046）；江西省自然科学基金资助项目（20161BAB212048）

作者简介：邓小鸿（1982-），男，副教授，博士，主要研究方向为网络信息安全（deng_xh@jxust.edu.cn）；梁涤青（1979-），男，讲师，博士，主要研究方向为混沌密码学；刘惠文（1987-），女，助教，硕士，主要研究方向为网络信息安全.

特性需要对区域进行表示[10]。基于频域的加密方法首先将医学图像从空域转换为频域，然后对选取的频域系数进行加密后进行逆变换得到加密图像，典型的方法如文献[11~13]。文献[11]提出了一种基于余弦变换和混沌映射的加密方法，具有较高的加密效率，但由于余弦变换涉及到浮点数运算，在不增加专门浮点运算硬件的情况下保证医学图像的加解密可逆性是不现实的。为了解决这一问题，Wu 等人[12]和梁涤青等人[13]均提出了基于整数小波变换和超混沌映射的加密方法，整数小波变换避免了系数运算中的浮点数问题，而超混沌映射提升了算法的安全性，算法仅对小波分解后的低频系数进行混沌加密，大大提高了加密效率，但超混沌序列的生成在时间效率上是瓶颈。由于频域系数与图像空域像素之间没有明确的对应关系，频域系数的改变往往会带来大量空域像素值的变化，选择频域系数进行图像加密具有较好的安全特性，在加密效率上高于空域算法。

综上所述，基于空域的加密算法相比频域方法，具有更高的加密性能，但加密效率较低；基于频域的方法仅对部分系数进行加密，为了提高算法的安全性，需要设计更加复杂的混沌映射，但超混沌系统的设计对算法的加密效率是挑战，并且通过对文献[13]进行实验分析发现，仅对低频系数进行加密，在医学图像存在明显边界的情况下加密图像中轮廓显现比较严重，算法的安全性降低。针对上述问题，本文提出基于 2D sine Logistic 混沌映射的医学图像频域加密算法，算法采用的 2D sine Logistic 混沌映射已经被证明具有超混沌系统特性，并且由简单的低维混沌系统组合而成，具有更加简单的系统结构。另外，对小波分解后的中高频子带进行简单的扩散加密，打破原有图像中边缘和纹理信息，解决加密图像中的轮廓问题。

1　相关知识与问题提出

1.1　整数小波变换

为了保证图像加解密的可逆性，采用基于提升方案的整数小波变换 LeGall5/3，该变换将整数映射到整数，并且小波的正变换和逆变换过程中保证了信息的无损性，是 JPEG200 压缩标准中指定的可逆小波变换[13]。设一个一维的信号 $s=[s_{0,1},s_{0,2},\cdots,s_{0,N}]$，其中 $s_{0,i}$ 为整数，可采用式(1)的小波正变换将信号 s 进行一级小波分级。

$$\begin{cases} d_{1,n}=s_{0,2n+1}-\lfloor 1/2(s_{0,2n}+s_{0,2n+2})+1/2\rfloor \\ s_{1,n}=s_{0,2n}+\lfloor 1/4(d_{1,n-1}+d_{1,n})+1/2\rfloor \end{cases} \tag{1}$$

其中：$d_{1,n}$ 为高频系数，$s_{1,n}$ 为低频系数，对于一级小波分级得到的低高频系数可以进一步利用式(1)进行更高级的分解，如 $s_{3,n}$ 代表三级小波分级的低频系数。对于二维的图像矩阵，可以把图像的行和列向量分别进行小波分解，对于分解后的系数矩阵，可采用式(2)的小波逆变换得到原始图像。

$$\begin{cases} s_{0,2n}=s_{1,n}-\lfloor 1/4(d_{1,n-1}+d_{1,n})+1/2\rfloor \\ s_{0,2n+1}=d_{1,n}+\lfloor 1/2(s_{j,n}d_{j,n}+s_{0,2n+2})+1/2\rfloor \end{cases} \tag{2}$$

其中：j 为分解级数。图 1 给出了图像三级小波分解后的频域系数子带和医学图像分解实例。每级小波分解得到四个频率子带，分别为 LL、HL、LH 和 HH，其中 LL 为低频子带，集中了原始图像的绝大部分能量，是原图的逼近子图，HL 和 LH 分别为垂直方向和水平方向的中高频子带，代表原图的纹理和边缘信息，为图像轮廓信息的主要集中地。

1.2　2D sine Logistic 混沌映射

一维的混沌系统具有更为简单的系统结构，但安全性能较差，如 Logistic 混沌系统已经证明存在着安全缺陷[14]。高维混沌系统具有更为复杂的系统结构和混沌性能，但实现费时。Hua 等人[15]将两个一维的混沌系统 Logistic 和 Sine 映射结合，提出了 2D sine Logistic 混沌映射，并且证明了其在安全性和实现效率上相比其他高维混沌系统具有优势。2D sine Logistic 混沌映射可表示为

$$\begin{cases} x_{i+1}=\alpha(\sin(\pi y_i)+\beta)x_i(1-x_i) \\ y_{i+1}=\alpha(\sin(\pi x_{i+1})+\beta)y_i(1-y_i) \end{cases} \tag{3}$$

其中：$x_i,y_i\in[0,1]$，$\alpha\in[0,1]$，$\beta\in[0,3]$，当 $\alpha\in[0.905,1]$ 并且 β 接近 3 时，2D sine logistic 混沌映射具有超混沌行为。

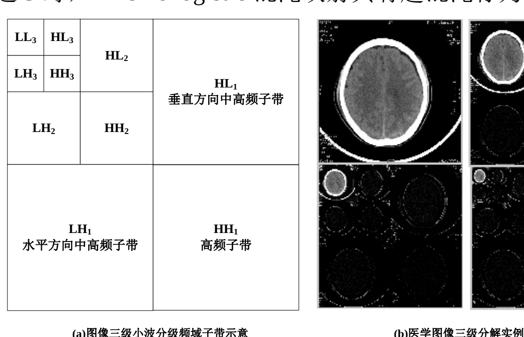


图 1　图像三级小波分级的系数子带及分解实例

Fig. 1　Coefficient subband of three-level wavelet transform and decomposition example of medical image

1.3　问题提出

文献[15]首先利用 2D sine Logistic 混沌映射生成混沌序列，然后利用混沌序列设计像素位置置乱和扩散算法，算法直接对图像的所有像素进行操作。表 1 给出了文献[15]方法在自然图像 Lena（不同的图像尺寸）中的测试结果，从表 1 中的结果可以看出，加密图像信息熵接近理想值 8，说明了算法良好的加密效果，但随着图像尺寸的增大，加密所需的时间大幅增加。虽然更优的实验环境可能带来更好的实验结果，但对于大数据量的医学图像来说，算法并不适用。一方面由于算法在空域进行，需要加密的数据量大，另外一方面由于设计的扩散和置乱算法过于复杂。

表 1　文献[15]方法在 Lena 中的测试结果

Table 1　Lena’s testing results in reference 15

载体图像	加密图像信息熵	加密时间/s	解密时间/s
Lena(128*128)	7.9882	0.610	0.594
Lena(256*256)	7.9972	8.14	8.09
Lena(512*512)	7.9993	40.044	41.538

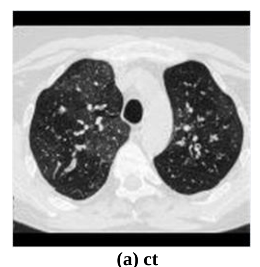
图 2 给出了载体图像 ct 采用文献[13]方法加密后的结果。文献[13]方法仅对三级小波分解的低频系数加密，从图 1 中可以看出，得到的图像出现明显的轮廓。事实上，通过实验分析，对于轮廓对比不分明的医学图像，文献[13]具有较好的加密效果，当医学图像中前景和背景区域对比度较大，呈现黑白分明时加密图像出现明显轮廓。加密图像中一旦存在原始图像的轮廓，会严重影响加密算法的安全，攻击者可以通过选择明文攻击来破译加密算法。

2　算法描述

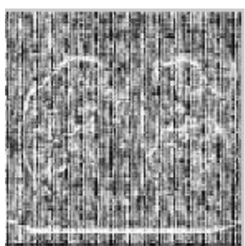
2.1　算法模型

本文算法模型如图 3 所示。算法首先将原始医学图像进行三级小波正变换，得到其系数矩阵，其中选取三级分解低频系数 LL_3 和二级分解中高频系数 LH_2 和 HL_2 作为待加密系数，其他系数保持不变；然后在给定混沌初值和参数情况下，利用 2D sine logistic 混沌映射生成混沌序列 1 和 2；接着将

系数 LL_3 利用序列 1 进行扩散加密，并将加密后的结果利用序列 2 进行置乱，将系数 LH_2 和 HL_2 利用序列 1 进行扩散加密，得到加密后的系数；最后将加密后的系数矩阵与其他未改变系数一起进行小波逆变换得到加密后的医学图像。解密过程是加密过程的逆过程，只需将原始医学图像改为加密医学图像，系数 LL_3 先进行混沌反置乱再进行混沌扩散，其他的步骤保持不变即可实现解密。算法在公开的网络环境下构建了一个安全的图像传输模型，图像的发送者和接收者协商密钥，并通过公钥密码体制进行安全传输，由于混沌加密体制具有大的密钥空间和强的初值敏感性，破译者在不知道密钥情况下仅从密文中无法破译出正确的图像信息。本文的创新之处将 2D sine logistic 混沌映射应用到了医学图像的小波域加密中，并设计了新的混沌扩散和置乱方法提高加密效率，同时选择对 LH_2 和 HL_2 系数进行置乱加密，有效解决了仅对低频系数加密而出现的图像轮廓问题。



(a) ct



(b) 文献[13]加密结果

图 2　加密效果对比结果

Fig. 2　Comparison results of encrypted efficiency

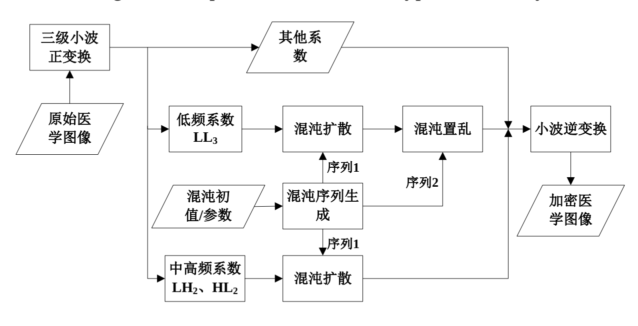


图 3　本文算法模型

Fig. 3　Model of the proposed algorithm

2.2　基于 2D sine logistic 的扩散和置乱算法

1) 扩散机制

设 seq_1 和 seq_2 分别为 2D sine logistic 混沌映射产生的混沌序列，其中 seq_1 用于对系数进行扩散，而 seq_2 用于对扩散后的系数进行位置置乱。设 coe 为原始医学图像整数小波分解后的系数集合，那么采用式(4)生成混沌密钥，采用式(5)前向反馈机制对系数进行扩散。

$$key(i)=\mathrm{mod}(round(seq_1(i)*10^5),256)\ i\in[0,len] \tag{4}$$

$$\begin{cases} e_coe(i)=\mathrm{mod}((coe(i)\oplus key(i))+key(i),256)\ if\ \ (i==0) \\ e_coe(i)=\mathrm{mod}((coe(i)\oplus key(i))+key(i-1),256)\oplus e_coe(i-1)\ else \end{cases} \tag{5}$$

其中：key 为密钥，e_coe 为加密后系数集合，len 为系数集合中元素的个数。mod 为取余函数，round 为四舍五入函数，$\oplus$ 为异或操作。

2)置乱机制

对于扩散后的系数采用式(6)进行置乱，改变系数位置。

$$\begin{cases} [sort_seq_2, location]=sort(seq_2) \\ e_coe'(i)=e_coe(location(i))\ \ i\in[0,M*N] \end{cases} \tag{6}$$

其中：$sort_seq_2$ 是对序列 seq_2 进行升序排序后的结果，$location$ 是排序后元素在原先序列中的位置，$sort$ 为升序排序函数，e_coe' 为对 e_coe 进行位置置乱后的结果。

基于 2D sine logistic 的扩散和置乱算法如算法 1 所示。

算法 1　根据生成的混沌序列对输入的系数进行扩散和置乱加密

输入：混沌序列集合 seq_1 和 seq_2，系数集合 coe

输出：加密系数集合 e_coe'

1. $e_coe'=coe$; //初始化为原系数集合
2. **for** i=1:len **do** //len 为集合长度
3. 　$seq_1(i)$=mod(round($seq_1(i)$*10^5),256);
4. end for
5. **for** i=1:len **do**
6. 　use the equation 5 to encrypt; //扩散加密
7. end for
8. [$sort_seq_2$,loc]=sort(seq_2);//对 seq_2 升序排序
9. **for** i=1:len **do**
10. 　$e_coe'(i)=e_coe(loc(i))$;//位置置乱
11. end for
12. output e_coe'

在算法 1 基础上，本文提出的医学图像频域加密算法如算法 2 所示。

算法 2　根据给定的混沌参数和原始医学图像得到加密医学图像

输入：混沌初值 $x0$,$y0$,控制参数 α 和 β,原始医学图像 I

输出：加密医学图像 EI

1. EI=I; //初始化为原始医学图像
2. [dim1, dim2]=size(I); //获取医学图像维数
3. Level=3;//设置小波分解的级数
4. decompose53(I, dim1, level);//小波正变换
5. N=dim1/(2^{level});
6. cof_LL=s33(1:N,1:N);//s33 为三级分解的低频系数
7. cof_HL=s22(1:N*2, N*2+1:2*N*2);//s22 为二级分级的低频系数
8. cof_LH=d22(1:N*2, 1:2*N);//d22 为二级分解的高频系数
9. [seq_1,seq_2]=D2_SLMM(α, β, $x0$, $y0$, 4*N*N);//D2_SLMM 为用式(3)生成混沌序列的函数
10. for a ∈ cof_LL do
11. 　调用算法 1 得到 e_cof_LL;
12. end for
13. for b ∈ cof_HL and c ∈ cof_LH do
14. 　调用算法 1 中置乱方法得到 e_cof_HL 和 e_cof_LH;
15. end for
16. s33(1:N,1:N)= e_cof_LL;
17. s22(1:N*2, N*2+1:2*N*2)= e_cof_HL;
18. d22(1:N*2, 1:2*N)= e_cof_LH;
19. EI=recompose53(I’, dim1, level);//小波逆变换
20. output EI;

3　实验结果与分析

实验中选取的 6 幅图像医学图像均来自于中南大学湘雅医学院，其中 4 幅尺寸为 512*512(x-ray、US、CT、MRI)，2 幅尺寸为 1024*1024(CT_foot 和 MRI_cervices)。实验主机配置环境：MATLAB 7.0，CPU 为 Intel(R) Core^{TM} i5-6500 3.20 GHz，内存 8 GB，64 位 Windows 7 旗舰版操作系统。实验中设定 2D sine Logistic 混沌的初值 $x0$=0.9380，$y0$=0.7006，控制参数 $\alpha=1$，$\beta=3$。

3.1　加密结果及分析

3.1.1 加密结果

采用本文算法对载体医学图像进行加密后的结果如图 4

所示。图 4 中(a)(c)(e)(g)(i)(k)分别为原始医学图像，(b)(d)(f)(h)(j)(l)为其对应的加密医学图像。从图 4 中所示结果来看，加密图像具有随机噪声分布特性，具有较好的加密效果，当加密图像未受到窜改和解密密钥与加密时保持一致时，能无损解密出原始医学图像。另外，对比图 2(b)和图 4(d)中结果，可以明显发现本文算法有效解决了加密图像中的轮廓问题。本文算法通过分析小波分解特点，选取二级小波分级后的中高频子带（代表了图像的纹理和边缘信息）进行加密，这样加密后的系数在进行小波逆变换时进行系数迭代和重构，充分掩盖图像的边缘信息。实验中同样对三级分解的中高频子带进行加密，发现效果不如二级系数明显，选用一级分解的中高频系数进行加密，虽然能较好地解决轮廓问题，但加密时间显著增加。

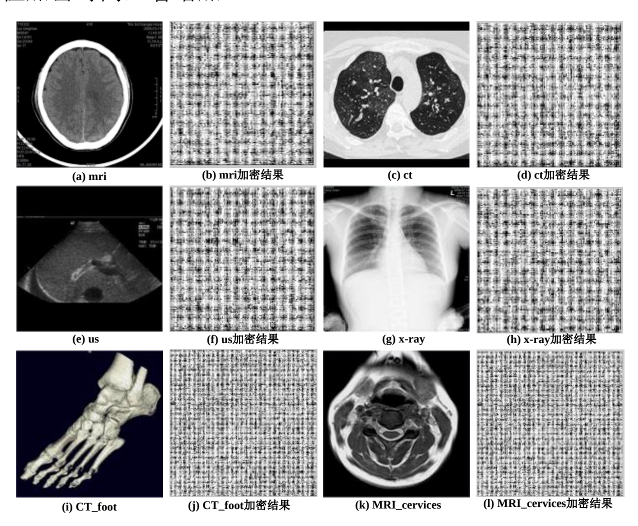


图 4　医学图像加密结果

Fig. 4　Encryption results of medical images

3.1.2 性能分析

1)密钥安全分析

密钥安全性主要通过密钥空间和密钥敏感性来衡量，密钥空间大小决定了攻击者采用穷举法进行暴力破解的难度，而密钥敏感性确保破译者不能使用与实际密钥相近的密钥恢复出原始信息。首先本文设计的密钥长度为 128 位(混沌初值和控制参数分别占 4 个字节，密钥位数为 4*32=128 位)，则密钥空间为 2^{128}，通过穷举搜索法破解密钥从计算上是不可能的。其次通过实验测试，将 2D sine logistic 混沌的初值 $x0$ 修改为 0.9381，其他的参数不变，采用该密钥去解密图像，得到的测试结果如图 5 所示。图 5 中，(a)为原始医学图像，(b)为采用默认密钥进行加密后的图像，(c)为采用修改密钥进行加密后的图像，(d)为(b)和(c)中图像求差的结果。从图 5(d)中可以看出，密钥的微小变化会造成加密结果的显著不同，另外采用修改后的密钥进行解密也无法得到原始的医学图像。

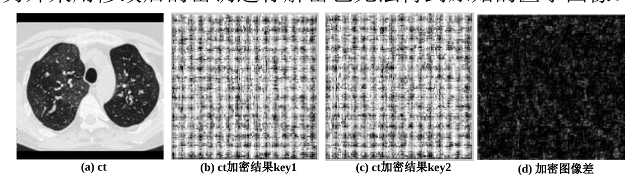


图 5　密钥敏感性结果

Fig. 5　The results of key sensitivity

2)抗统计攻击分析

加密图像信息熵和相邻像素相关性是定量衡量算法抗统计攻击的有效指标。图像信息熵表示图像灰度分布的统计特征，对于一幅类似随机噪声的加密图像，其灰度分布应该趋向于均匀化，其期望值应该为 8。信息熵和像素相关性计算公式如下：

$$Entropy = -\sum_{l=0}^{N} p(l)\log_2(p(l)) \tag{7}$$

$$corr = \frac{E[(X-\mu_X)(Y-\mu_Y)]}{\sigma_X \sigma_Y} \tag{8}$$

式(7)中，N 为像素值的灰度级数，$p(l)$ 为像素值 l 出现的概率。式(8)中，E 为求期望，X 和 Y 为两组数据序列，μ_X 和 μ_Y 分别为数据序列的均值，σ_X 和 σ_Y 为标准差。如果两个序列 X 和 Y 具有高的相关性，$corr$ 值接近于 1，相反接近于 0。经过计算，加密后的 6 幅图像的信息熵在 7.8 左右，接近于理想值 8。表 2 给出了载体图像 CT_foot 加密前后像素的相关性。从表 2 中结果可以看出，加密图像具有非常低的像素相关性。综上，本文加密算法能较好地抵抗统计攻击。

表 2　像素相关性测试结果

Table 2　Testing results of pixel correlation

载体图像	水平方向	垂直方向	对角线方向
CT_foot 原始图像	0.9988	0.9661	0.95942
CT_foot 加密图像	0.0017	-0.0034	0.0308

3)抗差分攻击分析

差分攻击是通过比较分析有特定区别的明文在通过加密后的变化传播情况来攻击密码算法。加密图像对明文的敏感性强度是衡量算法抗差分攻击的常用方法，通常利用式(9)中的像素改变率 $NPCR$ 计算。

$$\begin{cases} NPCR = \dfrac{1}{M*N}\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)\times 100\% \\ D(i,j) = (C_1(i,j) == C_2(i,j)\ ?: 1, 0) \end{cases} \tag{9}$$

其中：$M*N$ 为图像的尺寸，C_1 和 C_2 分别是两幅医学图像 I_1 和 I_2 对应的密文，其中 I_1 和 I_2 仅有一个像素值不同。

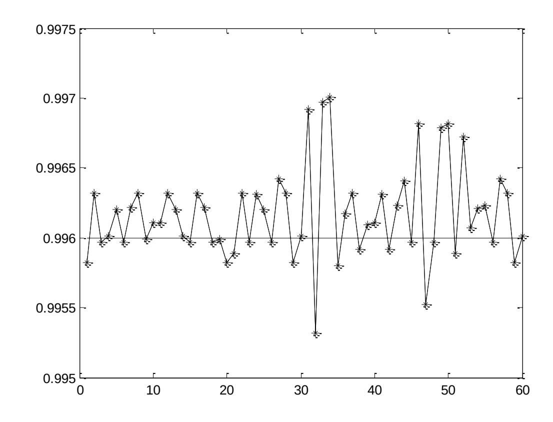


图 6　像素改变率测试结果

Fig. 6　Testing results of pixel changing rate

图 6 给出了 $NPCR$ 值测试结果。测试中选用 60 组医学图像(每副载体图像修改 10 个不同位置的像素点，与原图组成一组)，对每组进行编号，并随机选择每组进行加密，分别计算每组的 $NPCR$ 值。从图 6 中可以看出，像素改变率在理想值 0.996[13]上下波动，说明算法具有较强的抗差分攻击能力。

4)加解密效率分析

表 3 给出了 6 副载体图像加密和解密所需的时间，表中数据均是对图像加解密 10 次得到的平均结果。从表 3 中可以看出，当医学图像尺寸为 512*512 时，4 幅载体图像的加解密时间在 1.1 s 左右，当尺寸为 1024*1024 时，2 幅载体图像的加解密时间在 5s 左右，算法加解密效率较好。

表 3 本文算法加解密效率测试结果

Table 3 Encrypt efficiency testing results of the proposed algorithm

载体图像	加密时间/s	解密时间/s
x-ray(512*512)	1.129	1.131
us(512*512)	1.137	1.132
ct(512*512)	1.13	1.129
mri(512*512)	1.14	1.396
CT_foot(1024*1024)	4.966	4.847
MRI_cervices(1024*1024)	4.878	4.952

3.2 算法对比结果及分析

本文算法思路主要来源于文献[13,15]，实验结果主要与以上两个文献进行对比，对比的性能指标包括加密图像信息熵、加密时间和加密图像是否有轮廓。表 4 给出了本文算法和文献[13,15]的对比结果。从表 4 中结果可以看出，本文算法相比文献[15]方法，虽然加密图像信息熵较低，但在加密时间上具有明显优势，对于一副 M*N 的图像，文献[15]需要加密的像素个数为 M*N，而本文算法需要加密的系数个数仅为 $M*N(1/2^6+1/2^3)\approx M*N/8$。与文献[13]相比，本文算法的加密图像信息熵更接近于理想值 8，因为选取了更多的系数进行混沌加密，但加密时间上两个算法差不多，原因在于文献[13]方法生成超混沌序列的复杂度高于 2D sine logistic。除了信息熵外，本文算法最大的优势是解决了加密图像中的轮廓问题。

表 4 本文算法与其他对比方法的测试结果

Table 4 Comparison results between the proposed algorithm and other schemes

载体图像	文献[15]			文献[13]			本文算法		
	加密图像信息熵	加密时间 s	是否有轮廓	加密图像信息熵	加密时间 s	是否有轮廓	加密图像信息熵	加密时间 s	是否有轮廓
x-ray	7.998	41.256	无	7.792	1.096	无	7.803	1.129	无
us	7.997	40.977	无	7.794	0.997	无	7.812	1.137	无
ct	7.998	41.023	无	7.801	1.002	有	7.810	1.131	无
mri	7.996	41.144	无	7.800	1.078	有	7.825	1.145	无
CT_foot	7.999	198.56	无	7.796	5.002	有	7.799	4.966	无
MRI_cervices	7.998	199.87	无	7.795	4.993	有	7.803	4.878	无

4 结束语

网络环境下医学图像的安全传输需求日益增加，基于混沌的医学图像加密方法受到研究人员的广泛关注。本文在分析现有方法的基础上，充分考虑医学图像自身特点，提出了基于 2D sine Logistic 混沌映射的医学图像频域加密算法，设计了新的混沌扩散和置乱算法，对三级小波分解的低频系数进行加密，提高了算法的安全性和效率，另外为了解决加密图像中出现的轮廓问题，选取代表边缘和纹理信息的二级小波分级的中高频系数进行混沌扩散。实验结果表明本文算法在加密安全性和效率方面具有优势，算法适用于大数据量的医学图像实时加密。

参考文献：

[1] Cao Weijia J, Zhou Yicong, Chen C L P, *et al.* Medical image encryption using edge maps [J]. Signal Processing, 2017, 132(3): 96-109.

[2] Shabir A P, Frahana A, Javaid A S, *et al.* Hiding clinical information in medical images: a new high capacity and reversible data hiding technique [J]. Journal of Biomedical Informatics, 2017, 66(2): 214-230.

[3] Kumar C V, Natarajan V, Poonguzhali P. Secured patient information transmission using reversible watermarking and DNA encryption for medical images [J]. Applied Mathematical Sciences, 2015, 9(48): 2381-2391.

[4] Ravivhandran D, Praveenkumar P, Balaguru Rayappan J B, *et al.* Chaos based crossover and mutation for securing DICOM image [J]. Computers in Biology and Medicine, 2016, 72(5): 170-184.

[5] Singh L D, Singh K M. Medical image encryption based on improved ElGamal encryption technique [J]. Optik, 2017, 147(10): 88-102.

[6] Hua Zhongyun, Yi Shuang, Zhou Yicong. Medical image encryption using high-speed scrambling and pixel adaptive diffusion [J]. Signal Processing, 2018, 144(3): 134-144.

[7] Kanso A, Ghebleh M. An efficient and robust image encryption scheme for medical applications [J]. Communications in Nonlinear Science and Numerical Simulations, 2015, 24(1): 98-116.

[8] Moumen A, Bouye M, Sissaoui H. New secure partial encryption method for medical images using graph coloring problem [J]. Nonlinear Dynamics, 2015, 82(3): 1475-1482.

[9] Pareek N K, Patidar V. Medical image protecting using genetic algorithm operations [J]. Soft Computing, 2016, 20(2): 763-772.

[10] 邓小鸿，陈志刚，梁涤青，等. 分区域的医学图像高容量无损信息隐藏方法 [J]. 通信学报，2015, 36(1): 187-196. (Deng Xiaohong, Chen Zhigang, Liang Diqing, *et al.* Region-based lossless data hiding with high capacity for medical images [J]. Journal of Communications, 2015, 36 (1): 187-196.)

[11] Lima J B, Madeiro F, Sales F J R. Encryption of medical images based on the cosine number transform [J]. Signal Processing: Image Communication, 2015, 35(1): 1-8.

[12] Wu Xiangjun, Wang Dawei, Kurths J, *et al.* A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system [J]. Information Sciences, 2016, 349-350(C): 137-153.

[13] 梁涤青，陈志刚，邓小鸿. 基于超混沌映射的医学图像小波域加密算法[J]. 天津大学学报：自然科学与工程技术版 ，2016, 49(12): 1255-1261. (Liang Diqing, Chen Zhigang, Deng Xiaohong. Encryption method of medical image based on wavelet transform and hyper-chaotic mapping [J]. Journal of Tianjin University：Science and Technology, 2016, 49 (12): 1255-1261.)

[14] 陈志刚，梁涤青，邓小鸿，等. Logistic 混沌映射性能分析与改进[J]. 电子与信息学报，2016, 38(6): 1547-1551. (Chen Zhigang, Liang Diqing, Deng Xiaohong, *et al.* Performance analysis and improvement of logistic chaotic mapping [J]. Journal of Electronics & Information Technology, 2016, 38(6): 1547-1551.)

[15] Hua Zhongyun, Zhou Yicong, Pun C M, *et al.* 2D sine Logistic modulation map for image encryption [J]. Information Sciences, 2015, 297(C): 80-94.